IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF HP Laptop Computer, S/N 5CD7220T0S, CURRENTLY LOCATED AT the West Virginia State Police ICAC Unit Evidence Vault, Morgantown, WV	Case No. 1:20mj74

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, John Hare, Senior Inspector with the United States Marshal Service, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Senior Inspector with the United States Marshal Service (USMS). I have been employed with the USMS for over 27 years. I am currently assigned as the Northern District of West Virginia (N/WV) Sex Offender Investigation Coordinator. Among my duties, I am responsible for investigating crimes involving individuals who are convicted sex offenders and have failed to register under Title 18, U.S.C. § 2250(a).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that Jason Steven KOKINDA (KOKINDA) may be in violation of Title 18, U.S.C. § 2250(a), Failure to Register. On December 17, 2019, KOKINDA was indicted in the Northern District of West Virginia for Failure to Register in violation of Title 18, U.S.C. § 2250(a). During the course of this criminal investigation, it was learned that on September 30, 2019, the Elkins, WV Police Department executed a state search warrant on a vehicle belonging and being operated by KOKINDA. During the search of this vehicle, Elkins, WV Police Department seized a white in color **HP Laptop Computer, S/N 5CD7220T0S**. On October 1, 2019, the Elkins, WV Police Department obtained a state search warrant for the digital data and information accessible with the device. The Elkins, WV Police Department submitted the device to the West Virginia State Police ICAC Unit for forensics examination. Based on my training and experience and the facts as set forth in this affidavit, this device will provide information that will show KOKINDA traveled in interstate commerce from the State of New Jersey to the State of West Virginia and failed to register as a sex offender in the State of West Virginia as required by the Sex Offender Registration and Notification Act commonly known as SORNA, Title 18, U.S.C § 2250(a). There is probable cause to believe that the information described in Attachment A contains evidence of these crimes and items to be seized listed in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a **HP Laptop Computer, S/N 5CD7220T0S**, hereinafter the "Device." The Device is currently located at the West Virginia State Police ICAC Unit, Morgantown, WV.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. Beginning in early October 2019, the West Virginia State Police and the United States Marshal Service initiated a state/federal Failure to Register investigation into Jason Steven KOKINDA. KOKINDA had two prior felony sex offense convictions in the States of New Jersey and Pennsylvania. Based on these convictions, KOKINDA would be required to register as a sex offender under SORNA in the state of his residency.

8. On September 28, 2019, officers from the Elkins, WV Police Department were dispatched to the Elkins City Park in reference to a female juvenile being assaulted by an adult male. The complainant, a female juvenile advised the male subject had approached her at the park asking her for her Snap Chat and Tik Tok account names. The complaint advised the male touched her and began pushing her on the swings. The complainant stated the male had messaged her several times on Snap Chat. Investigating officers were able to document the Snap Chat conversations via screen shoot photo of the complainant's phone. This male was later identified as Jason Steven KOKINDA.

9. On September 29, 2019, KOKINDA was arrested by the Elkins, WV Police Department and charged with Obstructing an Officer, Fleeing on Foot, and Failure to Sign Fingerprint Card. The Ekins, WV Police Department later charged KOKINDA with Third Degree Sexual Abuse. It was later learned KOKINDA was an unregistered sex offender and had last registered in the State of Vermont in 2017.

10. On September 30, 2019, the Elkins, WV Police Department obtained a state search warrant for a 1999 Ford Contour bearing New Jersey registration C79LAH. This vehicle is registered to Jill Wong, mother of KOKINDA. During the execution of the search warrant, one Samsung cell phone, one HP Laptop Computer, S/N CND9044YXF; and one **HP Laptop, Computer S/N 5CD7220T0S** were seized as evidence.

11. On October 1, 2019, the Elkins, WV Police Department obtained a state search warrant for data contents located on the Samsung cell phone; the HP Laptop Computer, S/N CND9044YXF; and the **HP Laptop Computer, S/N 5CD7220T0S**. Those items were sent to the West Virginia State Police ICAC Unit in Morgantown, WV for forensic examination.

12. On October 2, 2019, the Elkins, WV Police Department contacted the West Virginia State Police to assist in their investigation. On this date, the West Virginia State Police obtained a state search warrant for the 1999 Ford Contour bearing New Jersey registration C79LAH. During the search, 7 credit cards belonging to KOKINDA, a black in color Alcatel cell phone, and one micro SD card were found.

13. SI John Hare was then contacted by the West Virginia State Police who requested assistance in a failure to register criminal investigation. During the initial investigation, SI Hare

and the West Virginia State Police found information that KOKINDA stayed at a camp site in Pendleton County, WV, from September 8, 2019, through September 22, 2019. SI Hare later developed information KOKINDA stayed at a camp site in Tucker County, WV, in late September 2019.

14. On October 23, 2019, the West Virginia State Police obtained state search warrants for the credit cards located in KOKINDA's vehicle. Records provided by the credit card companies showed KOKINDA had used the credit cards starting on August 23, 2019, at various locations in the Elkins, WV area and other places located within the Northern District of West Virginia up until his arrest on September 29, 2019.

15. As of April 16, 2020, the West Virginia State Police ICAC Unit has been unable to conduct any forensic examination on the submitted items due to extensive backlog of time sensitive investigations and lack of manpower.

16. The Device is currently in storage at the West Virginia State Police ICAC Unit in Morgantown, WV. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into their possession.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, as well as using a government-issued computer in my capacity as an USMS Senior Inspector, I know that the Device can access the Internet, store addresses and personal information, download pictures, download and share files, send and receive emails, has a video player, process and store data, has a GPS navigation device, and an IP address. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

By Phone

John Hare
Senior Inspector
United Sates Marshal Service

Subscribed and sworn to before me
on April 17, 2020:

MICHAEL JOHN ALOI
UNITED STATES MAGISTRATE JUDGE